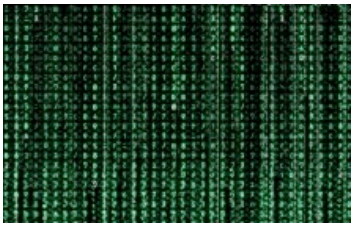
BIG BROTHER

La CIA espionne toutes vos données persos... et l'Europe s'en fiche

Philippe Vion-Dury | Journaliste Rue89
10/01/2013 à 16h54



Données, dans le film "Matrix" (Isaiah115/Flickr/CC)

Le gouvernement américain s'est octroyé depuis quelques années le droit d'espionner la vie privée des citoyens étrangers, dont les Européens, en mettant à contribution ses grandes compagnies, Facebook, Google ou Microsoft. Et les autorités européennes ferment les yeux.

C'est ce que dénonçait la version américaine de Slate le 8 janvier dernier, en s'apuyant sur le rapport [en anglais] "Combattre le cybercrime et protéger la vie privée sur le Cloud" du Centre d'études sur les conflits, liberté et sécurité, passé jusqu'alors tout à fait inaperçu.

La mise en place d'une sorte de tribunal secret, dont l'action ne se limite plus aux questions de sécurité nationale ou de terrorisme mais à "toute organisation politique étrangère", inquiète les auteurs de ce rapport remis au Parlement européen fin 2012.

Un risque pour la souveraineté européenne

Ceux-ci dénoncent le "Foreign Intelligence and Surveillance Act" (FISA), qu'ils accusent de "constituer un risque pour la souveraineté européenne sur ses données bien plus grave qu'aucune autre loi étudiée par les législateurs européens".

La loi FISA avait été introduite au Congrès en 2008 pour légaliser rétroactivement les mises sur écoute sans mandat auxquelles s'était livrée l'administration Bush dans le cadre de la lutte contre le terrorisme.

Malgré la polémique qu'il suscite encore, l'amendement a été prolongé en décembre dernier jusqu'en 2017, après que le Sénat l'a approuvé à 73 voix contre 23, tout en rejetant les amendements visant à placer des gardes-fous afin de prévenir d'éventuels abus.

Cette législation autorise expressément les agences de renseignement américaines (NSA, CIA...) à mettre sur écoute sans autorisation judiciaire des citoyens américains communiquant avec des étrangers soupçonnés de terrorisme ou d'espionnage.

"Carte blanche" pour espionner

Caspar Bowden, ancien conseiller sur la vie privée à Microsoft Europe et coauteur du rapport, accuse les autorités américaines d'avoir créé un outil de "surveillance de masse", en s'arrogeant le droit d'espionner les données stockées sur les serveurs d'entreprises américaines.

Pour simplifier, un tribunal secret est désormais capable d'émettre un mandat, secret lui aussi, obligeant les entreprises américaines (Facebook, Microsoft, Google...) à livrer aux agences de renseignement américaines les données privées d'utilisateurs étrangers.

Cette législation se démarquerait des autres en ne se limitant pas aux questions de sécurité nationale et de terrorisme, mais en l'élargissant à toute organisation politique étrangère ; une véritable "carte blanche pour tout ce qui sert les intérêts de la politique étrangère américaine" selon Bowden.

Cela pourrait inclure également la surveillance de journalistes, activistes et hommes politiques européens impliqués dans des sujets intéressant l'administration américaine.

L'inaction des responsables européens

Les auteurs soulignent l'inertie des responsables européens, qu'il trouve "choquante". Une inquiétude que partage Sophia in 't Veld, vice-présidente du Comité sur les libertés civiles, justice et affaires intérieures au Parlement européen, dont les propos sont rapportés par Slate :

> "Il est très clair que la Commission européenne ferme les yeux. Les gouvernements nationaux font de même, en partie parce qu'ils ne saisissent pas l'enjeu, et en partie parce qu'ils sont effrayés à l'idée d'affronter les autorités américaines."

Le renouvellement de la loi FISA et la publication de l'étude pourraient bien forcer les autorités européennes et nationales à se saisir de la question et à agir en conséquence. C'est en tout cas ce qu'espèrent les auteurs du rapport.

ALGORITHMES
13/07/2012 à 16h09

Comment Facebook lit vos messages privés (et peut les montrer à la police)

Martin Untersinger | Journaliste RueSG

Un homme tient une paire de jumelles (Gerlos/Flickr/CC)

Tout ce que vous écrivez sur Facebook – y compris la messagerie privée – est scruté par les ordinateurs de Facebook, à la recherche d'activités criminelles.

Si un comportement suspect – pédophilie, harcèlement... – est détecté par ses algorithmes, le cas remonte à l'équipe de sécurité du réseau social. C'est seulement à cette étape que des yeux humains se posent sur des discussions privées. Le cas échéant, le géant d'Internet se met en relation avec la police.

Toutes les entreprises surveillent ce qui se trame sur leur réseau. Mais une interview accordée à Reuters par Joe Sullivan, responsable de la sécurité à Facebook, est venue donner davantage de détails sur la manière dont Facebook a automatisé le processus de détection et comment, contrairement à d'autres géants, ce dernier est entièrement internalisé.

Une détection intelligente

Facebook se concentre en priorité sur les discussions supposées à risques. Le système accorde moins d'importance aux conversations entre deux membres qui ont l'habitude de discuter ensemble. En revanche, si deux membres ne sont pas amis, ont peu d'amis en commun, discutent pour la première fois et n'habitent pas dans la même zone, Facebook surveillera de plus près leurs échanges. Evidemment, les profils des mineurs font l'objet d'une attention particulière.

Mieux : les programmes de surveillance prennent également en compte des phrases utilisées dans leur chats Facebook par des délinquants interpellés par le passé.

Un sujet délicat

Facebook est généralement très discrète sur la façon dont elle surveille ses utilisateurs. D'abord parce que l'entreprise craint qu'on lui reproche son peu de précaution vis-à-vis de la vie privée (elle en a l'habitude). L'autre raison est avancée par Reuters : avec cette technologie, Facebook ne détecte que très peu de comportements anormaux.

L’interview de Reuters ne donne pas le nombre de cas transmis par Facebook aux services de police. Elle ne mentionne qu’un seul cas où Facebook est intervenu : un homme d’une trentaine d’années qui avait donné rendez-vous à une jeune fille de 13 ans au mois de mars. Mais Reuters cite "une demi-douzaine" d’officiers "louant" la manière dont "Facebook suscite des enquêtes".

"J’ai l’impression que pour chaque personne que nous arrêtons, dix autres passent à travers les mailles du filet", confirme à Reuters Jeffrey Duncan, de la police de Floride.

Joe Sullivan, le chef de la sécurité de Facebook, est évidemment très prudent :

> "Nous n’avons jamais voulu mettre en place un environnement dans lequel nos employés ont accès à des conversations privées, c’est donc très importants que nous utilisions une technologie de détection qui a un taux de faux positifs [fausses alertes, ndlr] très bas."

Dans sa communication officielle, Facebook ne parle pas de ce système : ni dans sa page destinée aux forces de l’ordre, ni dans le document confidentiel à l’intention des autorités de police et de justice, fuité fin 2011.

"La question, c’est la transparence de Facebook"

Raphaël Rault, avocat au cabinet BRM, rappelle que ce type de technologie n’est pas nouveau :

> "Les CGU [conditions générales d’utilisation, ndlr] du service utilisé peuvent prévoir ce “scan” des messages, à des fins de détection des comportements violents ou contraires aux bonnes mœurs. Quand on utilise un compte Gmail par exemple, un robot scanne nos e-mails pour proposer de la publicité ciblée."

Au niveau du droit, la détection automatique ne change pas vraiment la donne :

> "Il est possible d’avoir une modération automatique, basée sur des mots-clés par exemple, qui va systématiser le contrôle. Le code pénal, qui définit le statut des correspondances privées, s’applique, mais il faut également prendre en compte les finalités d’un tel traitement.
>
> Cela peut par exemple permettre au prestataire technique [ici, Facebook, ndlr] de ménager sa responsabilité : en France, on doit retirer un contenu manifestement illégal qui lui est signalé, y compris par un moyen automatique. La question, c’est la transparence, savoir si Facebook a informé ses utilisateurs."

NAVIGUEZ MASQUÉS
02/02/2012 à 12h33

Vie privée : le guide pour rester anonyme sur Internet

Martin Untersinger | Journaliste Rue89

1
Mis à jour le jeudi 2 février 2012 à 14h45

Hadopi, Acta : les lois qui surveillent Internet se multiplient. Mode d'emploi à l'usage des non-geeks pour utiliser le Web sans laisser de traces.

Un homme cagoulé (Instant Vantage/Flickr/CC)

Naviguer sur Internet, c'est comme sauter à pieds joints dans du béton frais : on laisse des traces (presque) indélébiles partout. C'est aussi ce que dit Bruce Schneier, expert en sécurité informatique :
"Si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris aux problèmes ni à la technologie."

L'informatique, et plus particulièrement Internet, est un formidable moyen de liberté d'expression, mais aussi une machine à surveiller. Or, surfer anonymement peut être souhaitable pour des tas de raisons, et pas seulement pour les paranos. On peut être amené à vouloir être anonyme sur Internet à un moment de sa vie. Liste non exhaustive et non exclusive :

1. échapper au flicage de son **patron** ;
2. éviter les yeux indiscrets de **sa femme/son mari** ;
3. déjouer la surveillance des **autorités** (cela ne vaut que si on habite dans un pays autoritaire, bien entendu), comme le font tant de dissidents, de la Biélorussie à la Syrie ;
4. empêcher de grandes entreprises – de préférence américaines – de collecter une foule de **données personnelles** ;
5. protéger **son travail ou ses sources** (si on est journaliste ou militant).

Renforcer son anonymat sur Internet, ce n'est pas "un truc de geek" : on dit souvent que la solution (ou le problème) se trouve entre la chaise et le clavier.

On peut agir, très simplement et toujours gratuitement, pour protéger sa vie privée et surfer anonymement sur Internet. Les solutions qui suivent ne sont pas à appliquer "en bloc", mais sont davantage un catalogue dans lequel piocher en fonction de ses besoins.

1

Le navigateur

L’historique

C’est parfois aussi simple que cela. La plupart des navigateurs stockent toutes les pages sur lesquelles vous vous rendez. Autant d’indiscrétions sur vos activités en ligne pour ceux qui ont accès à votre ordinateur (patron, conjoint(e)...).

Accessible dans les options ou en tapant Ctrl(Pomme)+H sur la plupart des navigateurs, il est également possible de supprimer l’historique avec le raccourci Ctrl(Pomme)+Maj+Suppr.

Les cookies

Ce sont des petits fichiers créés par certains sites que vous visitez et qui sont stockés dans votre navigateurs. Ils fourmillent (entre autres) de détails personnels : certains mémorisent l’identifiant et le mot de passe (afin que vous n’ayez pas à le ressaisir), d’autres stockent un panier d’achats sur un site d’e-commerce.

Ils sont autant de traces et vos passages sur le Web. Il est possible de les désactiver ou de les supprimer (via le menu "préférences" de votre navigateur).

La plupart des navigateurs modernes disposent d’une fonctionnalité qui permet de naviguer sans laisser de trace (historique et cookies). Mais attention, ce mode de connexion n’a aucun impact sur votre logiciel d’envoi d’e-mails ou de messagerie instantanée, seulement sur l’historique et les cookies de votre navigateurs.

2

La connexion

Pour afficher une page web, c’est le protocole HTTP qui est le plus souvent utilisé (oui, celui qui est dans votre barre d’adresse) : les données qui circulent avec ce protocole ne sont pas chiffrées.

Parfois, notamment sur les sites de commerce en ligne, un "s" vient s’ajouter au "HTTP" dans la barre d’adresse. Cela signifie que la communication entre votre ordinateur et le site web est chiffrée, donc beaucoup plus sécurisée.

Mais, afin d’éviter de voir son identité compromise sur Internet, cette précaution ne doit pas être cantonnée aux services de commerce en ligne. En 2010, un développeur mettait au point un petit programme, que l’on pouvait rajouter au navigateur Firefox, qui permettait par

exemple, notamment via le réseau WiFi, de dérober les identifiants Facebook ou Twitter de tous ceux qui se connectaient au réseau.

Une précaution simple pour éviter ce genre de déconvenues, l'installation de l'extension Firefox "HTTPS everywhere ", qui porte bien son nom : elle force tous les sites à communiquer avec votre ordinateur de manière chiffrée. Un bon moyen d'éviter que des yeux indiscrets sachent ce que vous faites avec votre connexion. Attention, certains sites n'autorisent pas une connexion sécurisée (vérifier le cas échéant la présence d'un petit cadenas dans la barre d'adresse ou celle du 's' après 'HTTP').

Cependant, la sécurité de la navigation en HTTPS réside dans des certificats, qui authentifient les sites utilisant cette technologie. Ces certificats sont de plus en plus volés et falsifiés, poussant même WikiLeaks à changer de système de soumission de ses documents confidentiels.

3

L'adresse IP

L'adresse IP est un élément central à comprendre afin d'être discret sur Internet.

C'est un peu **la carte d'identité de votre connexion Internet** (ce qui veut dire que plusieurs ordinateurs qui partagent la même connexion possèdent la même IP) : tous les sites ou services que vous visitez conservent une trace de votre connexion (plus ou moins longuement selon la législation du pays où ils sont implantés) – les 'logs' : il est donc possible de savoir qui s'est connecté, où et quand.

Lorsque vous laissez un commentaire ou postez une photo en ligne, l'adresse IP est 'mémorisée'. Les fournisseurs d'accès sont généralement capables de faire le lien entre une adresse IP et une identité bien réelle (en France, le délai de conservation des 'logs' est généralement d'un an).

Heureusement, plusieurs solutions existent pour se faire discret.

Le proxy

Un proxy est un ordinateur par lequel va transiter votre connexion, afin de masquer votre adresse IP.

Reporters Sans Frontières, dans son guide pour bloguer anonymement, explique (à travers l'exemple de Sarah, une fonctionnaire qui veut dénoncer les travers de son patron en utilisant un proxy) :

'Au lieu de se connecter directement à Hotmail.com, elle se connecte d'abord au proxy, qui lui-même se connecte à Hotmail. Quand Hotmail lui envoie une page, celle-ci est dans un premier temps reçue par le serveur proxy, qui la lui renvoie.'

C’est l’adresse IP du proxy, et non celle de son ordinateur qui est semée un peu partout sur Internet.

Le proxy présente quatre problèmes :

1. c’est le proxy qui **stocke les adresses IP** : ce qui n’est pas sans poser problème ;
2. un proxy se paramètre directement depuis son navigateur web ou **certaines applications** (e-mail, messagerie instantanée...) : ces dernières ne prévoient pas toutes cette fonctionnalité (il est cependant possible de les forcer à le faire) ;
3. la navigation devient plus **lente**, puisque la connexion fait sans cesse des aller-retours ;
4. les communications avec le proxy ne sont généralement **pas chiffrées**.

Une liste de proxys (ainsi que les moyens de les installer) est accessible sur cette plateforme collaborative.

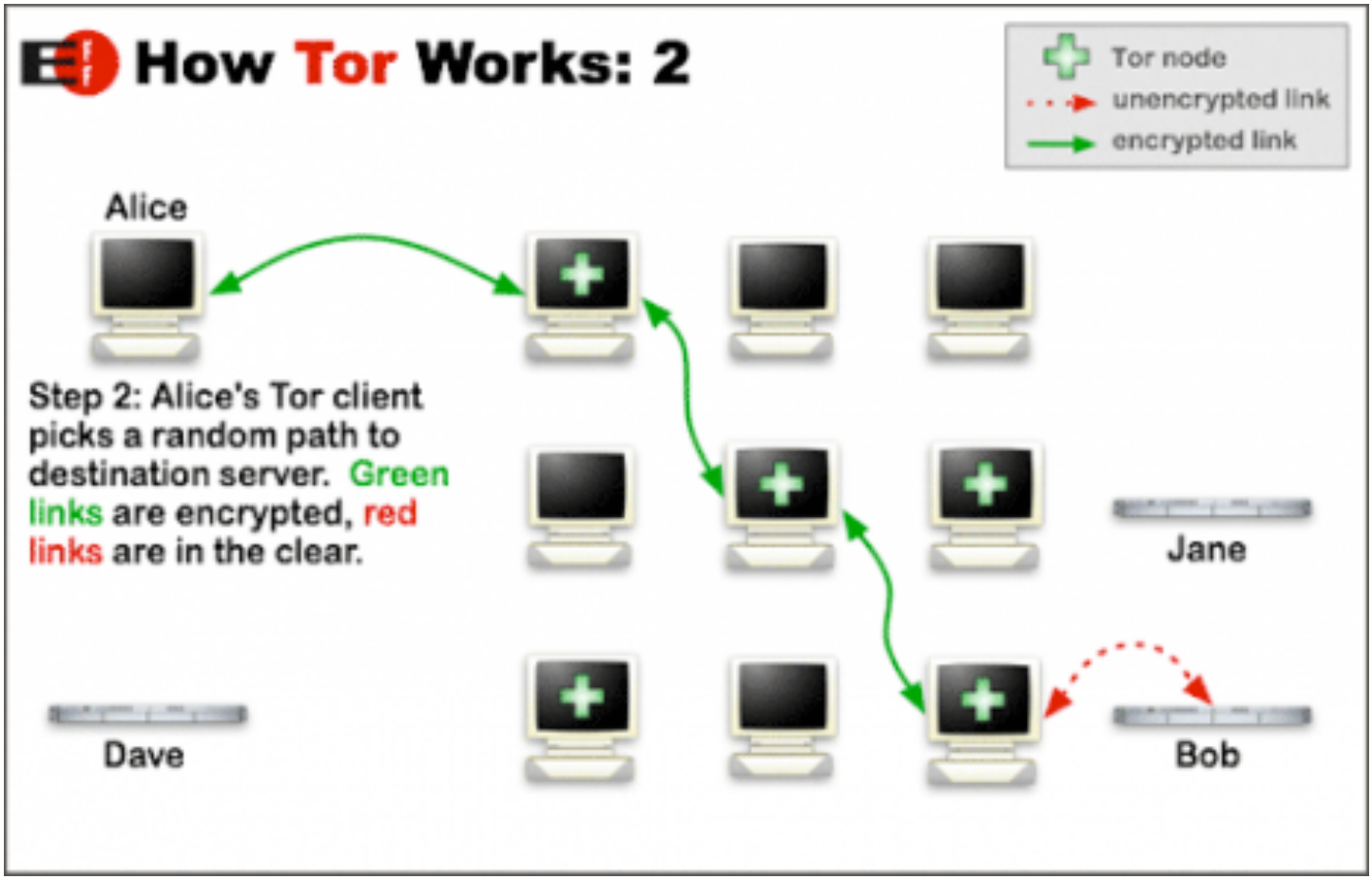

How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Schéma de fonctionnement de Tor (Torproject/CC)

Le réseau Tor

Tor est un réseau composé de multiples nœuds (ou couches, d’où son nom, qui signifie ‘oignon’ en anglais). Un ordinateur qui s’y connecte accède à Internet (sites web, mais aussi messagerie, mails...) à travers un ‘chemin’ tracé aléatoirement dans ces nœuds : cela permet de ne pas savoir d’où la connexion – chiffrée, bien évidemment – provient, ni ce qu’elle contient.

C’est un système souvent utilisé par les dissidents dans les pays où Internet est très surveillé.

Tor se présente sous la forme d'un logiciel assez facile à installer. Il est très largement utilisé dans les pays autoritaires, a même été financé par le gouvernement américain et a été utilisé par WikiLeaks. Problèmes :

1. la navigation utilisant ce logiciel est parfois lente ;
2. la sécurité de Tor n'est pas totale, et des failles ont été découvertes.

4

La cryptographie

Jusqu'à la toute fin des années 90, les logiciels de cryptographie étaient considérés comme une arme de guerre, et donc soumis à une régulation très stricte.
Depuis, n'importe qui peut chiffrer ses communications (e-mail, tchat, ou même ses fichiers et son disque dur tout entier).

Plusieurs solutions existent pour chiffrer ses communications.

La messagerie instantanée

De nombreux 'plugins' (petits modules qu'on ajoute à des logiciels) dit OTR ('off the record') permettent d'activer le chiffrement des communications.

Quelques logiciels sur lesquels cette fonctionnalité peut être activée : Adium, Pidgin, Miranda...

Les e-mails

Les e-mails sont très souvent surveillés. Même chose que pour la messagerie instantanée : des plugins peuvent être activés sur de nombreux logiciels, dont le célèbre Thunderbird.

La plupart du temps, c'est le logiciel PGP qui est utilisé et qui offre le rapport qualité/facilité d'utilisation le plus intéressant.

Les fichiers

Le logiciel TrueCrypt permet de chiffrer très facilement un fichier, un dossier ou même son disque dur tout entier.

C'est souvent l'algorithme AES, agréé par la NSA (un des services de renseignement des Etats-Unis) pour le chiffrement des informations top-secrètes du gouvernement américain, qui est utilisé. Officiellement, on commence à peine à trouver des failles à cet algorithme, réputé inviolable.

5

Précautions diverses

Un système d'exploitation ultra discret sur clé USB

Il est possible d'utiliser un ordinateur sans y laisser aucune trace. Tails est une variante du système d'exploitation Linux, qui combine les outils mentionnés précédemment pour chiffrer les e-mails et naviguer sur Internet anonymement.

Il se lance très simplement depuis un CD ou une clé USB, sans laisser la moindre trace de son passage sur l'ordinateur utilisé.

Les logiciels libres

De manière générale, pour renforcer sa confidentialité, il est conseillé de privilégier les logiciels libres. Leur code source est disponible et modifiable à souhait : les dizaines de milliers de programmeurs qui constituent la 'communauté du libre' ont décortiqué et analysé la plupart de ces logiciels.

Il y a donc beaucoup moins de chances que ces programmes contiennent des fonctionnalités 'malveillantes' comme des 'portes dérobées , qui pourraient menacer l'anonymat ou la sécurité. A l'inverse, seules les entreprises qui ont développé des logiciels dits propriétaires' ont accès aux codes sources de ces derniers.

Le site Framasoft entretient une liste de plus de 1 500 logiciels libres.

Les services payants et le 'cloud computing'

A des fins d'anonymat, il faut évidemment éviter tous les services qui exigent des coordonnées bancaires. Problème : beaucoup de services gratuits (comme Gmail ou Facebook) sont soumis au droit américain (et notamment à son Patriot Act), et peuvent être amenés, sur demande de la justice, à transmettre des données personnelles (à l'instar de Google, qui communique beaucoup sur cette question).

Beaucoup des services payants sont des services de 'cloud computing' – un terme à la mode. Ces techniques, qui consistent à héberger et à traiter des données en ligne plutôt que sur son propre ordinateur (Gmail ou Google Docs en font par exemple partie), sont évidemment à utiliser avec prudence.

Les données 'sur le cloud' ne vous appartiennent plus totalement, et vous n'avez pas une parfaite maîtrise sur qui en fait quoi et n'êtes pas à l'abri d'un bug ou d'une négligence.

Plusieurs identités numériques

Une autre précaution, si vous utilisez de nombreux services différents, est de recourir à un grand nombre de pseudos et d'adresses mail différentes, afin de rendre plus compliqué le croisement entre les bases de données et la compromission de l'anonymat.

Les métadonnées

Des détails contenus dans les fichiers Word, PDF, Excel ou les images peuvent compromettre l'identité du créateur du document ou de son émetteur.

C'est ce qu'on appelle les 'métadonnées' : ces dernières peuvent indiquer quel ordinateur a créé le document, quel logiciel a été utilisé, voire qui est son propriétaire ! Des moyens existent pour effacer [PDF] ces données peu discrètes.

Impossible d'être parfaitement anonyme

Ces précautions peuvent paraître inutiles. Pourtant, les menaces sur les libertés des internautes se sont multipliées :

1. la **DCRI** (contre-espionnage français) est capable de rentrer dans n'importe quel ordinateur ;
2. WikiLeaks a révélé la capacité de **certaines entreprises** à surveiller Internet à l'échelle d'un pays entier ;
3. et les initiatives comme Hadopi et Acta accroissent **la surveillance de l'Etat** et des entreprises sur les internautes.

Malgré toutes ces techniques, l'anonymat et plus généralement la sécurité informatique ne sont pas des notions absolues : il est impossible d'être parfaitement anonyme sur Internet, comme le note le journaliste spécialisé Jean-Marc Manach :
'La sécurité est un processus, pas un produit, et rien n'est pire qu'un faux sentiment de sécurité engendré par une accumulation de trucs' ou parce qu'on a acheté tel ou tel 'produit' ou logiciel de sécurité."

MERCI RIVERAINS ! Dosna, **Ben.Is.Nuts**, **Samuel Vimaire**, **raphael.w**, **Yru**, **rumpus**, **Lokiel**

INFOS PRATIQUES

Formation et rencontre entre journalistes et hackers

Le 25/02 à La Cantine

RSF, La Cantine, Silicon Maniacs, Reflets.info et Télécomix organisent une journée de formation et de rencontres entre journalistes et hackers le 25 février à La Cantine (151 rue Montmartre, Passage des Panoramas, Paris IIe). Journalistes et hackers discuteront des meilleurs moyens de se protéger sur Internet.

Ateliers de 13 à 18 heures (inscription obligatoire) suivi d'une table ronde de 18 à 20 heures (ouverte au public). Pour plus de renseignements et inscriptions aux ateliers : wefightcensorship@rsf.org.

16/03/2012 à 19h17

Tout voir, tout entendre : les espions en rêvaient, les USA l'ont presque fait

Martin Untersinger | Journaliste Rue89

Un œil à travers une loupe (Pink Sherbet/Flickr/CC)

Surveiller en temps réel l'intégralité des communications mondiales – Internet, téléphone, satellite –, même "cryptées", un rêve d'espion impossible ?

La NSA – l'agence américaine chargée du contre-espionnage, l'équivalent de notre DCRI – s'est lancée dans plusieurs projets qui vont lui permettre de réaliser ce rêve. C'est ce que révèle une longue enquête du magazine américain Wired, écrite par James Bamford, un des meilleurs spécialistes de la question.

Un gigantesque complexe

A Bluffdale, une bourgade de l'Utah de la banlieue de Salt Lake City, l'agence s'est lancée début 2011 dans la construction d'un complexe – top secret –, d'une ampleur totalement inédite, destiné à stocker et à analyser des quantités phénoménales de données. Les chiffres donnent le tournis :

1. un coût de deux milliards de dollars ;
2. une surface d'un million de m2, soit cinq fois la taille du Capitole à Washington ;
3. 10 000 ouvriers habilités "top secret" ;
4. une consommation électrique de 65 mégawatts (soit un quart de la puissance électrique consommée par Google) ;
5. plusieurs milliers de m2 de serveurs, parqués sous deux gigantesques hangars.

A compter de sa mise en service, programmée en septembre 2013, ce centre va être abreuvé des données recueillies par les satellites, les antennes à l'étranger et les postes d'écoute secrets de la NSA dispatchés sur tout le territoire américain.

L'objectif ? Etre capable de traiter des "yottabits" de données. Soit environ 1 000 milliards de fois plus que les disques durs de grande taille disponibles dans le commerce aujourd'hui. Bamford écrit :

> "Etant donné la taille des bâtiments et le fait qu'un terrabit de données peut désormais être stocké sur un disque grand comme le petit doigt, la quantité d'informations qui pourront être stockées à Bluffdale est réellement prodigieuse.

> Tout comme la croissance exponentielle de la quantité de données qui sont récoltées par la NSA et les autres agences."

Opération Vent stellaire

Bamford apporte de nouvelles informations concernant l'opération Vent stellaire, lancée en 2001 par la NSA afin de surveiller toutes les connexions Internet et téléphoniques entre les Etats-Unis et le reste du monde, mais aussi à l'intérieur du pays. Bamford explique que l'ampleur de la surveillance opérée par l'agence est bien plus grande qu'imaginée jusqu'ici :

> "L'opération Vent stellaire ne comportait pas seulement la surveillance des conversations téléphoniques, mais également l'inspection des e-mails."

William Binney, ancien mathématicien de la NSA, révèle à Wired que pour ce faire, l'agence a déployé sur tout le territoire des Etats-Unis des postes d'écoute, positionnés sur tous les nœuds importants d'Internet.

Il nous apprend également que la NSA utilise le "deep packet inspection" (DPI), une technique complexe qui permet d'inspecter le contenu de tout ce qui passe par le réseau : e-mails, messagerie instantanée (tchats), contenu des pages Internet consultées, notamment grâce à un logiciel développé par une filiale de Boeing. Bamford écrit :

> "Le logiciel cherche dans les e-mails des adresses précises, des lieux, des pays, des numéros de téléphone, des noms de personnes recherchées, des mots-clés, des phrases. Toute communication qui éveille les soupçons est automatiquement copiée, enregistrée."

"On est à ça d'un Etat totalitaire"

On apprend également que ce programme avait accès aux détails de facturations – l'équivalent des fameuses fadettes – du mastodonte des télécoms américain AT&T, ce qui lui permettait de savoir "qui appelait qui aux Etats-Unis et à travers le monde".

Binney a quitté la NSA pour protester contre la direction prise par l'agence. Peu avant, il lui avait suggéré d'adapter la surveillance des gens en fonction de leur proximité avec une cible.

La NSA a rejeté cette suggestion. "Ils stockent tout ce qu'ils récoltent", estime Binney.

Avec ces données, il est facile de tracer un portrait extrêmement fidèle d'un individu, explique-t-il : "On peut regarder tout le monde, tout le temps." Et d'ajouter :
"On est à ça d'un Etat totalitaire clé en main."

Un "super-ordinateur" top-secret

On connaissait l'existence du "jaguar ", ce super-ordinateur lancé en 2004, classé un temps comme le plus puissant au monde (aujourd'hui dépassé par un ordinateur chinois).

Mais on apprend dans l'article de Wired que la NSA a également mené un projet parallèle, un super-ordinateur top secret bien plus puissant que son homologue public, achevé en 2006.

Cryptographie : ‘Une énorme percée’

On apprend (encore) que, dotée de cette puissance de calcul sans équivalent dans le monde, la NSA s’est lancée dans une course que tout le monde croyait perdue d’avance : parvenir à casser les systèmes de chiffrage (la terminologie correcte pour ce qu’on appelle généralement ‘cryptage’) de données les plus complexes jamais conçus.

L’un d’eux – appelé AES – est aujourd’hui réputé inviolable. La NSA elle-même l’a adoubé. Il est aussi l’un des plus utilisés (par les services secrets, les entreprises, les activistes, les terroristes...). Et l’auteur de nous apprendre que l’agence américaine a récemment établi une ‘énorme percée’ dans ce domaine... sans préciser laquelle. Il explique :

> ‘Le super-ordinateur secret de la NSA est modifié spécialement pour la crypto-analyse, et utilisé pour déchiffrer un ou plusieurs algorithmes spécifiques, comme l’AES.’

C’est ainsi que les pièces du puzzle se mettent en place. Jamais rêve d’espion n’avait été aussi proche de la réalité : des capacités de stockage dantesques, des super-ordinateurs d’une puissance inouïe, des sources de données quasi-illimitées et des technologies de chiffrage susceptibles d’être cassées.

Les contre-espions américains sont ‘à ça’ de pouvoir surveiller, intercepter, analyser et comprendre toutes les télécommunications qui transitent sur la planète.

Image de page d’accueil : Anarchosyn/Flickr/CC.